Lesley E. Weaver (SBN 191305)
lweaver@bfalaw.com
Anne K. Davis (SBN 267909)
adavis@bfalaw.com
Joshua D. Samra (SBN 313050)
jsamra@bfalaw.com
BLEICHMAR FONTI & AULD LLP
1330 Broadway, Suite 630
Oakland, California 94612
Tel.: (415) 445-4003
Fax: (415) 445-4020

Sabita J. Soneji (SBN 224262)
ssoneji@tzlegal.com
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, California 94612
Tel.: (510) 254-6808

Counsel for Plaintiffs and the Proposed Class

[Additional counsel on signature block]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JOSEPH JACKSON and RACHEL ZIMMERMAN, individually and on behalf of all similarly situated persons,

Plaintiffs,

v.

THE ALLSTATE CORPORATION, ALLSTATE INSURANCE COMPANY, ALLSTATE VEHICLE AND PROPERTY INSURANCE COMPANY, ARITY, LLC, ARITY 875, LLC, and ARITY SERVICES, LLC,

Defendants.

Case No. 3:25-cv-00894

CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiffs Joseph Jackson and Rachel Zimmerman, individually and on behalf of all others similarly situated ("Plaintiffs"), bring this Class Action Complaint against The Allstate Corporation, Allstate Insurance Company, Allstate Vehicle and Property Insurance Company, Arity, LLC, Arity 875, LLC, and Arity Services, LLC (collectively, "Defendants"). Plaintiffs allege the following facts based upon personal knowledge, investigation by counsel, and on information and belief:

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendants seeking to redress the harms caused by Defendants' surreptitious, and unconsented, collection of Plaintiffs' personal information. The consumer driving data Defendants collected is highly invasive and personal, including information about what consumers did inside their cars each and every time they drove or rode in a vehicle sufficient to "fingerprint" (*i.e.*, identify) each individual driver. The data Defendants harvested from each consumer was tied to individuals and included geolocation, route history, driving schedule, fuel or charging levels, hard braking events, hard acceleration events, tailgating, time spent idle, speeds over 80 miles per hour, vehicle speed, average speed, late night driving, driver attention, and more (hereinafter, "Driving Data"). Defendants collected consumer Driving Data from consumers' own mobile devices, in-car devices and apps, and the vehicles they drove—without consumers' knowledge or consent—and then used that personally identifying information for their own purposes (including to calculate insurance rates for Plaintiffs) or sold the data to third parties for profit.

2. Defendants Allstate Insurance Company and Allstate Vehicle and Property Insurance Company are all insurance companies and are subsidiaries of and owned by Defendant The Allstate Corporation (collectively, the "Allstate Defendants"). The Allstate Defendants sell vehicle insurance policies to individual consumers, pricing their insurance policies based on factors such as the driver's age, where they live, what type of vehicle they drive, and their driving record. Consumers provide this information to Allstate Defendants when they apply for an insurance policy.

3. Defendants Arity, LLC, Arity 875, LLC, and Arity Services, LLC (collectively, the "Arity Defendants") are all technology companies and are subsidiaries of and owned by Defendant The Allstate Corporation. Arity Defendants collect personal information from consumers via its

websites, third-party mobile apps, Arity's own mobile app, Arity's software development kit ("SDK"), or via devices installed in consumers' vehicles.[1]

4. Together, Defendants conspired to collect and sell the driving behavior data of at least 40 million consumers, totaling "one trillion miles of driving data."[2]

5. Defendants collected this data in part by developing and embedding their own software into third-party apps. Once a consumer downloaded one of those apps onto their phone, Defendants' software was downloaded as well, enabling Defendants to maintain a connection with the consumer's phone, whether the consumer wanted it or not. Using the embedded software, Defendants could monitor the consumer's location and behavior in real time and by pulling a trove of personal data directly from the consumer's phone.

6. In order to ensure their software was included in third-party apps, Defendants paid app developers millions of dollars to integrate Defendants' SDK into the third-party apps. Defendants also provided bonuses to these app developers as an additional incentive to participate in this integration. The success of Defendants' efforts to expand the reach of their software can be seen in their own claim that their software enables them to "capture[] [data] every 15 seconds or less" from "40 [million] active mobile connections."[3]

7. The personal data collected by Defendants included information that together would be used to create a profile of a consumer's driving behavior, such as their phone's geolocation data, as well as accelerometer data, magnetometer data, and gyroscopic data, which monitors details such as the phone's altitude, longitude, latitude, bearing, GPS time, speed, and accuracy.

8. Defendants also harvested additional identifying information, including first and last name, phone number, address, zip code, mobile ad-ID ("MAID"), and device ID (together, "Identity Information").

[1] ARITY, "Privacy Statement," (effective date: November 1, 2024), https://arity.com/privacy/ (last accessed on Jan. 27, 2025).

[2] ARITY, https://arity.com/ (last accessed on Jan. 27, 2025).

[3] ARITY, https://arity.com/solutions/real-time-insights/ (last accessed on Jan. 27, 2025).

9. Defendants used the Driving Data and Identity Information (together, "Personal Data") to build a driving behavior database consisting of the "largest driving behavior dataset tied to insurance claims," which they used to both support and expand their own insurance business and to sell to third parties for profit.[4]

10. Defendants marketed and sold the Personal Data obtained through third-party apps as "driving" data purportedly reflecting consumers' driving habits. The Personal Data, however, was and is fundamentally flawed.

11. For example, the Personal Data was used and sold as "driving" data despite the fact that the data was collected from, and in reality, reflected the location and movement of consumers' phones—not the consumer's driving behavior. Thus, Defendants collected the consumer's data and attributed it to individuals regardless of whether that individual was in fact operating a vehicle at that time. For example, Defendants collected and reported data as reflecting an individual's driving behavior even when the individual was riding as a passenger in a motor vehicle, or even riding a rollercoaster.

12. The Driving Data was and is further decontextualized from the ways that vehicle owners can and must safely operate their vehicles. For example, a "hard braking event" may in fact be a safe and appropriate response to driving conditions—if, for example, a child or animal suddenly enters the roadway—but such an event could still have a negative impact on the individual's risk score, as assigned by Defendants.

13. Defendants have recently begun to expand the sources of their data by buying vehicle data directly from car manufacturers. This additional trove of data will allow Defendants to better distinguish between data reflecting the location and movement of a consumer's phone and data reflecting the location and movement of a particular vehicle.

14. Defendants used this Personal Data to make insurance coverage decisions for consumers who sought vehicle insurance with them. They would also sell this data to other insurers, enabling those insurers to make their own coverage decisions about individual consumers.

[4] ARITY, *supra* n.2.

Defendants and other insurers used consumers' Personal Data to decide whether to market insurance products to individual consumers, and how much to increase a consumer's insurance premium or whether to provide them with insurance at all. These decisions were made without the consumer's knowledge that their Personal Data had been collected and used by Defendants to affect their insurance coverage.

15. Consumers were not informed of and did not consent to this collection of their Personal Data.

16. The putative Class is comprised of millions of Americans who were not informed of, did not consent to, and suffered harms as a result of Defendants' ongoing collection, use, and sale of their Personal Data. Plaintiffs and Class Members seek compensatory, consequential, statutory, punitive, general, and nominal damages, disgorgement and restitution, and injunctive relief on behalf of all consumers whose data was captured, collected, stored, and sold by Defendants without their knowledge and consent.

II. PARTIES

A. Plaintiffs

17. **Plaintiff Joseph Jackson** is a resident and citizen of the state of California who, at all material times, resided in Santa Rosa, California.

18. Plaintiff Jackson is a customer of the Allstate Defendants, from whom he purchases auto insurance for three of his vehicles. Plaintiff Jackson has been a customer of the Allstate Defendants for the last five (5) years.

19. Plaintiff Jackson has the SiriusXM in-car app, in which Defendants' Arity SDK is embedded, in two of his vehicles. One vehicle has had the SiriusXM app for about eight years, and the other vehicle for about one year.

20. Plaintiff Jackson's cellphone has the mobile app Life360, in which Defendants' Arity SDK is embedded. Plaintiff Jackson has had the Life360 app on his cellphone for about four years.

21. Unbeknownst to Plaintiff Jackson, upon information or belief, Defendants intercepted and collected his Personal Data through his Life360 mobile app and SiriusXM apps.

22. Plaintiff Jackson did not consent to his Personal Data being collected through his Life360 mobile app or Sirius XM apps, nor did he consent to it being shared with Defendants.

23. Plaintiff Jackson incurred harm as a result of Defendants' invasion of his privacy, taking his data in which he has a property right, and diminishing the value of his data. Further, upon information and belief, Plaintiff Jackson suffered from increased premiums paid to the Allstate Defendants as a result of his Personal Data being provided without his consent to Defendants.

24. **Plaintiff Rachel Zimmerman** is a resident and citizen of the state of Illinois who, at all material times, resided in Naperville, Illinois.

25. Plaintiff Zimmerman was a customer of the Allstate Defendants, from 2020–2024, from whom she purchased auto insurance.

26. Plaintiff Zimmerman's cellphone has the mobile app GasBuddy, in which Defendants' Arity SDK is embedded. Plaintiff Zimmerman has had the GasBuddy app on her cellphone for about five years.

27. Plaintiff Zimmerman's cellphone has the mobile app Fuel Rewards, in which Defendants' Arity SDK is embedded. Plaintiff Zimmerman has had the Fuel Rewards app on her cellphone for about five years.

28. Unbeknownst to Plaintiff Zimmerman, upon information and belief, Defendants intercepted and collected her Personal Data through her GasBuddy and Fuel Rewards apps.

29. Plaintiff Zimmerman did not consent to her Personal Data being collected through her GasBuddy Fuel Rewards app, nor did she consent to it being shared with Defendants.

30. Plaintiff Zimmerman incurred harm as a result Defendants' invasion of her privacy, taking her data in which she has a property right, and diminishing the value of her data. Further, upon information and belief, Plaintiff Zimmerman suffered from increased premiums paid to the Allstate Defendants as a result of her Personal Data being provided without her consent to Defendants.

B. Defendants

31. **Defendant The Allstate Corporation** is a United States public corporation headquartered in Glenview, Illinois, and incorporated under the laws of Illinois. Together with its

subsidiaries, Defendant The Allstate Corporation provides insurance products, including car insurance, throughout the United States.

32. **Defendant Allstate Insurance Company** is a wholly owned subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Insurance Company provides insurance products, including car insurance, throughout the United States.

33. **Defendant Allstate Vehicle and Property Insurance Company** is a subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Vehicle and Property Insurance Company provides insurance products, including car insurance, throughout the United States.

34. **Defendant Arity, LLC** was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Chicago, Illinois, and it is incorporated under the laws of Delaware. Defendant Arity, LLC is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, and uses predictive analytics to build solutions to sell to third parties.

35. **Defendant Arity 875, LLC** was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Northbrook, Illinois, and it is incorporated under the laws of Delaware. Upon information and belief, Arity 875, LLC's members, including Allstate, Alexandra Band, Christopher Belden, Jennifer Brown, Julie Cho, Eric Ferren, Amit Goswami, Suren Gupta, Gary Hallgren, Christina Hwang, and Lisa Jillson, are all citizens of Illinois. Defendant Arity 875, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, and uses predictive analytics to build solutions to sell to third parties.

36. **Defendant Arity Services, LLC** was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Northbrook, Illinois, and it is incorporated under the laws of Delaware. Upon information and belief, Arity Services, LLC's members, including Allstate, Alexandra Band, Christopher Belden, Jennifer Brown,

Julie Cho, Eric Ferren, Amit Goswami, Suren Gupta, Gary Hallgren, Christina Hwang, and Lisa Jillson, are all citizens of Illinois. Defendant Arity Services, LLC is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, and uses predictive analytics to build solutions to sell to third parties.

III. JURISDICTION AND VENUE

37. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interests and costs, and this is a class action in which one or more members of the proposed class, including Plaintiff Jackson, are citizens of a state different from Defendants. The Court has supplemental jurisdiction over the alleged state law claims under 28 U.S.C. § 1367 because they form part of the same case or controversy.

38. This Court has personal jurisdiction over the Defendants as Defendants have sufficient minimum contacts with California, including but not limited to their continuous and systematic business activities within the state.

39. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in the District.

IV. GENERAL FACTUAL BACKGROUND

40. Defendants' driving behavior dataset is drawn from "130M+ average daily trips from 45M+ active geographically dispersed consumer connections," *i.e.*, more than 45 million Americans.[5] Defendants gathered this data directly from consumers, without their knowledge and consent, and have used consumers' data to make insurance coverage decisions and generate profit for themselves and for other insurers.

[5] ARITY, "Benefits," https://arity.com/solutions/vehicle-miles-traveled/ (last accessed on Jan. 27, 2025).

A. Defendants Developed Software Tools to Covertly Collect Consumers' Location Data

41. On information and belief, in 2015 Defendants designed an SDK that could be integrated into third-party mobile phone applications to collect data about the location and movements of a person's phone. SDKs usually consist of pre-built components, including software, APIs, libraries, and instructions to help developers in building software applications.

42. Defendants' SDK, however, was created as little more than a means for Defendants to siphon user data from third-party apps. Specifically, the Arity SDK was designed by Defendants to collect immense amounts of data related to the location and movements of a consumer's phone directly from the consumer's phone.

43. Once incorporated in a mobile app, the Arity SDK harvested several types of data, including but not limited to:

a. a mobile phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data;

b. "Trip attributes," which included information about a consumer's movements, such as start and end location, distance, duration, start and end time, and termination reason code;

c. "GPS points," such as the accuracy, position, longitude, latitude, heading, speed, GPS time, time received, bearing, and altitude of a consumer's mobile phone;

d. "Derived events," such as acceleration, speeding, distracted driving, crash detection, and attributes such as start and end location, start and end time, speed attribute, rate of change attribute, and signal strength attribute; and

e. Metadata, such as ad ID, country code, iOS vs. Android indicator, User ID, device type, app version, and OS version.

44. Meanwhile, consumers who had chosen to download and use a third-party app had no knowledge that the app they were using also contained the Arity SDK, which was harvesting their data. Defendants never notified nor otherwise informed consumers that they were collecting their data via the Arity SDK and third-party apps.

45. The Driving Data, even without the Identity Information, can be personally identifying. For example, the data collected just from the accelerometer of a mobile device can create an "accelerometer fingerprint" that can permit the receiver of that data to "track [a user] over space and time."[6] One study found that, once created, such a "fingerprint" is "hard to erase, unless the accelerometer wears out to the degree that its fingerprint becomes inconsistent"—which was not observed even once during 9 months of testing 107 different accelerometers.[7]

B. Defendants Paid App Developers to Integrate the Arity SDK into Mobile Apps

46. Since at least 2017, Defendants have paid third-party app developers millions of dollars to integrate the Arity SDK into their respective mobile apps. Defendants successfully integrated Arity SDK into several popular apps, such as Routely, Life360, GasBuddy, Sirius XM, Fuel Rewards, Streewise, GPS Driving Route, Fuelzee, and Ago. These apps had a key feature that made them appealing to Defendants as a vehicle for their data collection efforts: all these apps required location information to function properly. Location information is central to the development of the Personal Data Defendants sought to capture, since it factors into many components of driver data, such as geolocation, "trip attributes," "GPS points," and "derived events."

47. Once an app integrated the Arity SDK, a consumer who downloaded and used that app unknowingly enabled Defendants to collect their location data without their consent.

48. In addition, Personal Data collected from users by the third-party apps was licensed to and shared with Defendants. The personal data that mobile apps licensed to Defendants generally included first and last name, phone number, address, zip code, mobile ad-ID ("MAID"), and device ID. Together with the Driving Data, the Personal Data could be used by Defendants to more reliably identify the specific person being monitored by the Arity SDK.

49. Defendants would similarly share some of the driving data they collected with the third-party apps with which they contracted to support those apps' features. Thus even the third-party

[6] Dey at al., "AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable" at 2, *available at* https://www.ndss-symposium.org/wp-content/uploads/2017/09/03_2_1.pdf.

[7] *Id.*

apps that consumers chose to download and use for a specific purpose profited from Defendants' surreptitious and nonconsensual collection of consumers' personal information.

C. Defendants' Products and Services Monetized Class Members' Personal Information

50. Defendants further profited off the Personal Data they collected by using it to create and sell additional products and services. These products and services included:

a. **Drivesight**. Drivesight is a product created and sold by the Arity Defendants to generate a driving score for potential insureds by analyzing data and using that information to score that individual's driving risk.[8]

b. **ArityIQ**. This product is directed at insurers, enabling them to access the driving data collected by Defendants and to use that data to assign more accurate (and therefore "to price more profitably") insurance rate quotes to individual consumers."[9]

c. **Arity Marketing Platform**. Defendants' marketing platform enables third-party advertisers to target drivers "based on driving behavior data" and publishers to "monetize their inventory by displaying relevant ads to high-intent US drivers at scale."[10]

d. **Arity Audiences**. Defendants let companies, including third-party insurers, target drivers with marketing "based on their actual driving history." As part of this product, Defendants displayed ads to the users of apps that agreed to integrate the Arity SDK.[11]

e. **Real Time Insights**. This product collects and distributes transportation-related data derived from the personal and driving data collected by Defendants.

---

[8] ARITY, "Drivesight®," https://arity.com/solutions/drivesight/ (last accessed on Jan. 27, 2025).

[9] ARITY, "ArityIQ SM," https://arity.com/solutions/arity-iq/ (last accessed on Jan. 27, 2025).

[10] ARITY, "Arity Marketing Platform," https://arity.com/solutions/arity-marketing-platform/ (last assessed on Jan. 27, 2025).

[11] ARITY, "Arity Audiences," https://arity.com/solutions/arity-audiences/ (last accessed on Jan. 27, 2025).

f. **Routely**. This product is offered to consumers as a "free" application providing "helpful insights" into the consumers' driving habits to encourage safer driving. By contrast, Defendants sell this product to insurers as "a better way to effectively measure and quantify risky driving behaviors" and "provide personalized pricing while lowering loss ratios."[12]

51. Notably, Defendants primarily marketed the Driving Data to third parties as "driving behavior" data as opposed to what the Driving Data really was: data about the movements of a person's mobile phone. On information and belief, Defendants had no way to reliably determine whether a person was driving at the time Defendants collected the Driving Data, or which particular person was driving.

52. For example, if a person was a passenger in a bus, a taxi, or a friend's car, and that vehicle's driver sped, braked hard, or made a sharp turn, Defendants would conclude that the passenger, not the actual driver, engaged in "bad" driving behavior based on the Driving Data. Defendants would then subsequently sell and share the data so it could be used to inform decisions about that passenger's insurability based on their "bad" driving behavior.

53. In a further example of Defendants' abusive practices in connection with Driving Data, a person's driving score was lowered because the "driving" behavior data collected from his phone claimed he was driving, when he was actually riding a roller coaster.[13]

54. The Driving Data further would not reflect contextual information necessary to determine whether certain driving events recorded reflected risky driving. A "hard braking event," for example, could be the result of a sudden hazard such as a child or animal running into the roadway. But the Driving Data would record only a "hard braking event," negatively impacting the risk score assigned by Defendants.

[12] ARITY, "Routinely®," https://arity.com/solutions/routely/ (last accessed on Jan. 27, 2025).

[13] Chad Murphy, "Sir, this is a roller coaster. Car insurance dings driving score for man riding The Beast." THE CINCINNATI ENQUIRER (October 8, 2024), https://www.cincinnati.com/story/entertainment/2024/10/08/insurance-cutsdriving-score-man-riding-the-beast-kings-island/75554987007/.

55. These flaws are and should have been obvious to all of the Defendants, yet they continued to collect, disclose, and profit from flawed Driving Data without regard to inaccuracy of the information.

D. Defendants' Failure to Disclose the Collection, Sharing, and Use of Plaintiffs' Driving Data

56. Pursuant to their agreements with app developers, Defendants had varying levels of control over the privacy disclosures and consent language that app developers presented to consumers. However, neither Defendants, nor the apps running Defendants' Arity SDK, informed Plaintiffs and Class Members that Defendants were collecting Personal Data, or purported to do so in a confusing and/or opaque manner. Nor did Defendants, nor the apps on Defendants' behalf, inform Plaintiffs and Class Members of the various ways that Defendants would collect, use, and ultimately monetize the Personal Data collected by Defendants.

57. Because Defendants did not disclose their unlawful practices, Plaintiffs and Class Members were wholly unaware that Defendants were collecting the Personal Data from their phones. Plaintiffs and Class Members were likewise wholly unaware (and had no way of knowing) that Defendants would use the Personal Data to create and sell several different products and services to third parties, including other insurers.

58. Defendants did not provide Plaintiffs and Class Members with any sort of notice of their data and privacy practices, nor did the mobile apps notify consumers about Defendants' practices on Defendants' behalf. Similarly, neither Defendants nor the mobile apps notified consumers of the ways in which their Driving Data would be used, nor did consumers agree to have their data used for Defendants' own products or services.

59. Even if a Class Member took the extra step to investigate Defendants outside of their app, navigated to Defendants' website, and located their privacy disclosures, they would still not understand what Defendants did with their data. Consumers reading Defendants' privacy disclosures are met with a series of untrue and contradictory statements that do not reflect Defendants' practices.

60. For example, Arity's Privacy Policy states that it "do[es] not sell personal information for monetary value,"[14] which is untrue. Defendants sold a number of data-based products and services for monetary value that linked a specific app user to their alleged driving behavior. Further, Defendants do not provide Class Members with the ability to request that Defendants stop selling their data.

61. Defendants likewise obscured how they used Plaintiffs' and Class Members' data. In Defendants' privacy disclosures, Defendants state that they "[u]se [consumers'] personal data for analytics and profiling." But in describing how Defendants "profile" consumers, Defendants fail to explain that they combine the Driving Data and Personal Data to create a database of driving profiles for more than 45 million Americans and selling access to said database. Rather, Defendants describe their profiling activities as follows:

> We use your personal data to assist in our development of predictive driving models. We may profile [consumers'] personal data only for the purposes of creating a driving score ('Driving Score'), which is used for our analytics purposes to develop and validate our predictive driving models.[15]

62. In the event a Class Member took the extraordinary steps of tracking down Defendants' privacy statement, finding the subparagraph describing profiling, parsing through Defendants' convoluted description of their profiling activities, and concluding that they did not want Defendants to use their data to create a "Driving Score" about them, the Class Member still could do nothing to stop Defendants from collecting their data and creating a Driving Score. Defendants did not describe, nor provide, a method for a consumer to request that their data not be used to profile them.

E. Defendants' Practices Cause Substantial Injury to Consumers

63. As set forth above, the Arity SDK is capable and may be used to identify individual consumers and their visits to sensitive locations. Specifically, Defendants' actions caused economic harm to Plaintiffs who paid more for insurance as a result of the information collected about them.

[14] ARITY, "Privacy Statement," *supra* n.1.

[15] *Id.*

Plaintiffs were also economically harmed because the information taken from them without consent has an economic value that can be measured by the very markets for that data the Arity Defendants participate in. Where someone works, lives, shops, spends time, congregates, and travels are all used to infer information about someone's interests and demographics, data that is of high value.

64. Defendants' actions also constituted significant privacy harms. Defendants' surveillance of Plaintiffs' activities within their vehicles—which for many Americans is private space where they spend a considerable amount of time speaking with others and engage in intimate actions beyond simply driving—is an unlawful intrusion in and of itself. Collection and sale of such data is an intrusion into the most private areas of a consumer's life. The scope, quality, and character of the data collected must also be considered as part of that harm.

F. Plaintiffs' Injuries

Plaintiff Jackson

65. As set forth above, unbeknownst to Plaintiff Jackson, Defendants intercepted his Personal Data through his Life360 mobile app and SiriusXM apps.

66. On information and belief, the Arity SDK harvested Personal Data from Plaintiff Jackson without his knowledge or consent.

67. Plaintiff Jackson did not consent to his Personal Data being collected through his Life360 mobile app or Sirius XM apps, nor did he consent to it being shared with Defendants.

68. Plaintiff Jackson incurred harm as a result Defendants' invasion of his privacy, taking his data in which he has a property right, and diminishing the value of his data. Further, upon information and belief, Plaintiff Jackson suffered from increased premiums paid to the Allstate Defendants as a result of his Private Data being provided without his consent to Defendants.

Plaintiff Zimmerman

69. As set forth above, unbeknownst to Plaintiff Zimmerman, Defendants intercepted her Personal Data through her GasBuddy and Fuel Rewards apps.

70. On information and belief, the Arity SDK harvested Personal Data from Plaintiff Zimmerman without her knowledge or consent.

71. Plaintiff Zimmerman did not consent to her Personal Data being collected through her GasBuddy Fuel Rewards app, nor did she consent to it being shared with Defendants.

72. Plaintiff Zimmerman incurred harm as a result Defendants' invasion of her privacy, taking her data in which she has a property right, and diminishing the value of her data. Further, upon information and belief, Plaintiff Zimmerman suffered from increased premiums paid to the Allstate Defendants as a result of her Personal Data being provided without her consent to Defendants.

V. TOLLING OF THE STATUE OF LIMITATIONS

73. All applicable statute(s) of limitations have been tolled by Defendants' knowing and active concealment and denial of the facts alleged herein. Plaintiffs and Class Members could not have reasonably discovered Defendants' practice of surreptitiously acquiring and compiling their sensitive location data without their consent, selling it to third parties, and/or compiling it in a manner that impacts their insurance premiums—including when the data gathered does not accurately reflect Plaintiffs or Class Members' driving habits.

74. Defendants were and remain under a continuing duty to disclose to Plaintiffs and Class Members their practice of acquiring sensitive location data for use in determining insurance premiums. As a result of the active concealment by Defendants, any and all applicable statutes of limitations otherwise applicable to the allegations herein have been tolled.

VI. CLASS ACTION ALLEGATIONS

75. Plaintiffs seek certification of the class set forth herein under Federal Rule of Civil Procedure 23. Specifically, Plaintiffs seek class certification of all claims for relief herein of a class and subclass defined as follows:

> **Class:** All persons residing in the United States and its territories whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Class").
>
> **California Subclass**: All person residing in California whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "California Subclass")
>
> **Illinois Subclass**: All person residing in Illinois whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Illinois Subclass")
>
> **FCRA Subclass**: All persons residing in the United States and its territories whose vehicle Driving Data and/or Identity Information was collected, stored, distributed,

and/or sold by Defendants, and for which a report was created, which was then disclosed to a third party.

76. Excluded from the proposed Class are: Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

77. Plaintiffs reserve the right to re-define the Class definition after conducting discovery.

78. **Numerosity (Fed. R. Civ. P. 23(a)(1)).** The Class Members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes millions of people who were harmed as a result of Defendants' unlawful conduct. The parties will be able to identify the exact size of the Class through discovery and Defendants' records.

79. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3)).** Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but are not limited to the following:

a. Whether Defendants engaged in the activities and practices referenced above, including whether Defendants collected and shared Plaintiffs' and Class Members' Driving Data;

b. Whether Defendants used this information to determine insurance premiums and/or insurance coverage;

c. Whether Plaintiffs and Class Members consented to such collection and sharing;

d. Whether Defendants were unjustly enriched;

e. Whether Defendants' conduct constitutes an invasion of privacy and/or an intrusion upon seclusion;

f. Whether Defendants' conduct violated federal and state wiretap laws;

g. Whether Defendants acted knowingly and/or willfully;

h. Whether Plaintiffs and Class Members sustained damages as a result of Defendants' activities and practices referenced above, and, if so, in what amount;

i. Whether Defendants should be enjoined from such conduct in the future; and

j. Whether Defendants profited from their activities and practices referenced above, and, if so, in what amount.

80. All members of the proposed Class are readily ascertainable. In the Driving Data and Personal Data they surreptitiously collected, Defendants have access to the addresses and other contact information for members of the Class, which can be used for providing notice to many Class Members.

81. **Typicality (Fed. R. Civ. P. 23(a)(3)).** Pursuant to Rule 23(a)(3), Plaintiffs' claims are typical of the claims of the Class Members. Plaintiffs' claims are typical of the claims of the members of the Class because all Class Members' highly personal data was captured by Defendants in the same or substantially similar way, and thus Class Members were similarly harmed as a result.

82. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)).** Pursuant to Rule 23(a)(4), Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class Members. Plaintiffs have retained counsel experienced in prosecuting class actions and data privacy cases.

83. **Superiority (Fed. R. Civ. P. 23(b)(3)).** Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Class Members because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

84. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because:

a. the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual

Class Members which would establish incompatible standards of conduct for Defendants;

b. the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to individual Class Members which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

c. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

85. **Issue Certification (Fed. R. Civ. P. 23(c)(4)).** In the alternative, the common questions of fact and law, set forth in Paragraph 79, are appropriate for issue certification on behalf of the proposed Class.

VII. CAUSES OF ACTION

COUNT I
VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. §§ 2510, *et seq.*
(On Behalf of Plaintiffs and the Class Against All Defendants)

86. Plaintiffs repeat and fully incorporates all preceding paragraphs as if fully set forth herein.

87. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

88. In relevant part, the FWA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

89. The FWA also makes it unlawful for any person to intentionally disclose, or endeavor to disclose, to any other person or to intentionally use, or endeavor to use, the "contents of any wire, oral, or electronic communication, knowing or having reason to know that" the communication was obtained in violation of the FWA. 18 U.S.C. § 2511(1)(c) & (d).

90. The FWA provides a private right of action to any person whose wire, oral, or electronic communication is intercepted, used, or disclosed. 18 U.S.C. § 2520(a).

91. The FWA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

92. The FWA defines "electronic communication" as "any transfer of signs, signals, […] data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

93. The FWA defines "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

94. The FWA defines "contents," with respect to any covered communication, to include "any information concerning the substance, purport, or meaning of that communication[.]" 18 U.S.C. § 2510(8).

95. The FWA defines "person" to include "any individual, partnership, association, joint stock company, trust, or corporation[.]" 18 U.S.C. § 2510(6).

96. Defendants are each a person as defined in 18 U.S.C. §2510(6).

97. The data and transmissions within, to, and from Plaintiffs' and Class Members' mobile devices constitute "electronic communications," as defined by 18 U.S.C. § 2510(12), as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photooptical systems that affect interstate commerce.

98. As alleged herein, Defendants intercepted, in real time, contemporaneously, and as it was transmitted, the contents of electronic communications transmitted within, to, and from Plaintiffs' mobile devices and third-party apps, and diverted those communications to themselves without consent.

99. As detailed herein, the electronic communications detailed above that Defendants have intercepted are tied to individual drivers and vehicles, and not anonymized.

100. Plaintiffs and Class Members have a reasonable expectation of privacy within their vehicles, and Plaintiffs and Class Members reasonably expected privacy while driving their vehicles and using their mobile devices.

101. Common understanding and experience of how mobile apps work create a reasonable expectation that an insurer and its affiliates, such as Defendants, would not surreptitiously intercept and divert the detailed and personal electronic communications described above.

102. In further violation of the FWA, Defendants have intentionally used or endeavored to use the contents of the electronic communications described above knowing or having reason to know that the information was obtained through interception in violation of 18 U.S.C. § 2511(1)(a). 18 U.S.C. § 2511(1)(d).

103. Specifically, Defendants used the illicitly obtained information to price insurance products sold to Plaintiffs and Class Members and sold this information to other insurers.

104. As a result, Plaintiffs and Class Members have suffered harm and injury due to the interception, disclosure, and/or use of electronic communications containing their private and personal information.

105. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class Members have been damaged by Defendants' interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made by Defendants as a result of the violation or (b) statutory damages for each Class Member of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT II
VIOLATION OF THE STORED COMMUNICATIONS ACT, 18 U.S.C. §§ 2710, *et seq.*
(On Behalf of Plaintiffs and the Class Against All Defendants)

106. Plaintiffs repeat and fully incorporates all preceding paragraphs as if fully set forth herein.

107. Plaintiffs and Class Members specifically restate the allegations relating to the elements and definitions under the FWA/ECPA set forth above.

108. The Federal Stored Communications Act ("SCA") creates a civil remedy for those whose stored electronic communications have been obtained by one who "intentionally accesses without authorization" or "intentionally exceeds an authorization to access" a facility through which an electronic communication service ("ECS") is provided. 18 U.S.C. §§ 2701, 2707.

109. "Electronic communication" is defined as "any transfer of signs, signals, . . . data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

110. "Electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (incorporated by reference in 18 U.S.C. § 2711(1)).

111. "Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication . . . ." 18 U.S.C. §§ 2510(17) (incorporated by reference in 18 U.S.C. § 2711(1)).

112. Plaintiffs, as individuals, and Defendants, as corporations or legal entities, are "persons" within the meaning of 18 U.S.C. § 2510(6), and for purposes of 18 U.S.C. § 2707.

113. The electronic communications transmitted within, to, and from Plaintiffs' and Class Members' mobile devices are stored in electronic components of those devices.

114. In-device components with storage function are facilities through which electronic communication services are provided because they provide users, such as Plaintiffs and Class Members, the ability to send and receive electronic communications.

115. As alleged herein, there is a reasonable expectation of privacy within a person's vehicle and while using their mobile device, and Plaintiffs and Class Members reasonably expected privacy.

116. Defendants, without the consent or authorization of Plaintiffs or Class Members, accessed certain data stored in consumers' mobile devices and transmitted it to their servers via cellular network throughout a trip, at the completion of a trip, or on some other periodic basis.

117. Defendants accessed these temporarily stored electronic communications in addition to and separately from intercepting other electronic communications transmitted in real time.

118. Defendants intentionally accessed each of these facilities without authorization.

119. Defendants intentionally exceeded its authority to access these facilities.

120. In accessing these facilities without authorization and obtaining access to the electronic communications stored there, Defendants violated the SCA, 18 U.S.C. § 2701.

121. Defendants' conduct was willful and intentional, and invaded Plaintiff's and Class Members' expectations of privacy.

122. The communications accessed by Defendants in violation of the SCA have significant value, evidenced by the profits that Defendants have obtained from, among other things, licensing and selling the improperly accessed communications.

123. Pursuant to 18 U.S.C. § 2707, Plaintiffs and Class Members have been damaged and aggrieved by Defendants' intentional acts in violation of the SCA and are entitled to bring this civil action to recover declaratory and equitable relief; damages in an amount to be determined at trial, assessed as actual damages and any profits made by Defendants as a result of the violation, but in no case less than $1,000; reasonable attorneys' fees and other litigation costs reasonably incurred; punitive damages as determined by the Court.

COUNT III
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §§1030, *et seq.*
(On Behalf of Plaintiffs and the Class Against All Defendants)

124. Plaintiffs repeat and fully incorporate all preceding factual allegations as if fully set forth herein.

125. The Computer Fraud and Abuse Act ("CFAA"), enacted in 1986 as part of the ECPA, prohibits the intentional accessing, without authorization or in excess of authorization, of a computer under certain circumstances. 18 U.S.C. § 1030(a).

126. The CFAA specifically provides that it is unlawful to "intentionally access a computer without authorization or exceed[] authorized access, and thereby obtain[]…information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

127. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality and privacy of information within their computers.

128. The CFAA specifically provides that it is unlawful to "intentionally access a computer without authorization or exceed[] authorized access, and thereby obtain[]…information from any protected computer." 18 U.S.C. § 1030(a)(2)(c). 1039.

129. Plaintiffs, as individuals, and Defendants, as corporations or legal entities, are "persons" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(12).

130. A "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(10).

131. "Exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain." 18 U.S.C. § 1030(e)(6).

132. Plaintiffs and Class Members' mobile devices are data-processing devices performing logical, arithmetic, and storage functions and thus constitute a "computer" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(1).

133. A "protected computer" is defined as "a computer . . . which is used in or affecting interstate or foreign commerce or communication…, [or that] has moved in or otherwise affects interstate or foreign commerce." 18 U.S.C. § 1030(e)(2)(B). Plaintiffs' and Class Members' mobile devices are used to send and receive information and electronic communications across state lines and internationally. Thus, they constitute "protected computers" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(2)(B).

134. Through their SDK embedded in third party apps, Defendants intentionally accessed the Plaintiffs' and Class Members' mobile devices without Plaintiffs' or Class Members' authorization, or in a manner that exceeded Plaintiffs' and Class Members' authorization, and obtained information therefrom in violation of the CFAA. 18 U.S.C. § 1030(a)(2)(C).

135. Plaintiffs and Class Members have suffered harm and injury due to Defendants' unauthorized access to the communications containing their private and personal information.

136. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I) from the unauthorized access and collection of Driving Data to Plaintiffs and Class Members and excessive insurance costs. Plaintiffs and the Class are entitled to bring this civil action and are entitled to economic damages, compensatory damages, injunctive, equitable, and all available statutory relief, as well as their reasonable attorney's fees and costs and other relief as permitted by the CFAA. 18 U.S.C. § 1030(g).

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class Against All Defendants)

137. Plaintiffs hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

138. Plaintiffs and Class Members have a common law, legally protected privacy interest in their driving data and are entitled to the protection of their information and property against unauthorized access.

139. Plaintiffs and Class Members reasonably expected their driving behavior, tendencies, and characteristics would not be collected and shared by Defendants without their express consent. This data includes sensitive information about Plaintiffs' and Class Members' personal lives, including where they drove, when, and where.

140. Defendants unlawfully invaded the privacy rights of Plaintiffs and Class Members by: (a) collecting their Personal Data in a manner that is highly offensive to a reasonable person; and (b) disclosing their Personal Data amongst each other and with unauthorized parties without the informed and clear consent of Plaintiffs and Class Members

141. In intentionally collecting sharing Plaintiffs and Class Members' Personal Data, Defendants acted in reckless disregard of their privacy rights, intruded into their seclusion, and publicly disclosed their private data.

142. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiffs and Class Members' private, personal, and confidential information has been accessed or

is at imminent risk of being accessed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and Class Members have suffered injuries as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

143. Plaintiffs and Class Members are entitled to actual damages, punitive damages, and compensatory damages for invasion of their privacy in an amount to be determined by a jury at trial.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class Against All Defendants)

144. Plaintiffs hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

145. Plaintiffs bring this claim on their own behalf and on behalf of Class Members.

146. Defendants collected and sold Plaintiffs' and Class Members' Personal Data, without Plaintiffs' and Class Members' consent to insurance companies and to other third parties and also used it to build products and services. Defendants also used this data to evaluate insurance premiums and coverage.

147. Plaintiffs and Class Members received no benefit from this use and sale of their Personal Data. Indeed, because Plaintiffs and Class Members did not consent to Defendants' collection and sale of Plaintiffs' and Class Members' Personal Data, they could not and do not benefit from such practices. It is therefore inequitable for Defendants to retain any profit from such collection and sale without payment to Plaintiffs and Class Members for the value of their Personal Data.

148. Defendants are therefore liable to Plaintiffs and Class Members for restitution in the amount of the benefit conferred on Defendants as a result of its wrongful conduct, including specifically the value to Defendants of the Personal Data that they wrongfully intercepted, collected, used, and sold to third parties, and the profits Defendants received or is currently receiving from the use and sale of that Personal Data.

COUNT VI
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT
(On Behalf of Plaintiffs and the FCRA Subclass Against Defendant Arity Services, LLC)

149. Plaintiffs hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

150. Plaintiffs bring this claim on their own behalf and on behalf of each member of the FCRA Subclass described above against Defendant Arity Services, LLC.

151. Plaintiffs and FCRA Subclass Members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

152. Under the FCRA, a "consumer reporting agency" includes any person which, for monetary fees or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other consumer information for the purpose of furnishing "consumer reports" to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. At all relevant times, Defendant Arity Services, LLC was a consumer reporting agency. 15 U.S.C. § 1681a(f).

153. Under the FCRA, a "consumer report" is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used, expected to be used, or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for (i) credit or insurance to be used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) any other purpose authorized by 15 U.S.C. § 1681b. At all relevant times, Defendant Arity Services, LLC had compiled and maintained "consumer reports" on Plaintiffs and FCRA Subclass Members. 15 U.S.C. § 1681a(d)(1).

154. As consumer reporting agencies, Defendant Arity Services, LLC is and was required to identify, implement, maintain, and monitor systems to ensure the accuracy of consumer information in its possession, custody, and control, including Plaintiffs' and FCRA Subclass Members' Driving Data.

155. Defendant Arity Services, LLC obtains driver behavior data from Defendants and furnishes it to third parties, including automobile insurers, without Plaintiffs' and other FCRA Subclass Members' full knowledge and consent.

156. Defendant Arity Services, LLC's provision of credit information that includes driver behavior data to third parties, including automobile insurance companies, constitutes the furnishing of consumer reports under the FCRA and an impermissible purpose and use of data under the FCRA.

157. The FCRA requires credit reporting agencies to adopt reasonable procedures to ensure the "maximum possible accuracy" of the consumer credit information it furnishes. 15 U.S.C. § 1681e(b).

158. Defendant Arity Services, LLC, acting as a consumer reporting agency, as defined by 15 U.S.C. § 1681c(1), has failed to implement procedures to maintain "maximum possible accuracy" regarding Plaintiffs' and FCRA Subclass Members' Driving Data.

159. Defendant Arity Services, LLC has knowingly and willfully engaged in the collection and production of inaccurate data metrics regarding Plaintiffs' and FCRA Subclass Members' driving abilities. Those actions have included, among other things as alleged herein:

a. Adopting and implementing systems which misreport Driver Data and as being associated with one individual, when that information should be associated with other individuals;

b. Continuing to misreport Driver Data and Identity Information even when Defendant Arity Services, LLC knows that the systems developed to collect and report such information is prone to errors, does not correctly report Driver Data, provides no context for certain Driver Data, and is not subject to review to ensure that the Driver Data is correct;

c. Preparing reports which Defendant Arity Services, LLC knew, or was reckless in not knowing, that the Driver Data included therein was inaccurate.

160. As a result of Defendant Arity Services, LLC's conduct, insurance carriers and others who view these consumer reports receive and in turn rely on an inaccurate representation of Plaintiffs' and FCRA Subclass Members' driving abilities.

161. The foregoing deceptive acts and practices constitute reckless and/or negligent violations of the FCRA, including, but not limited to, 15 U.S.C. § 1681e(b).

162. As a result of each and every willful violation of the FCRA, Plaintiffs are entitled to actual damages as the Court may allow pursuant to 15 U.S.C. § 1681n(a)(1); statutory damages pursuant to 15 U.S.C. § 1681n(a)(1); punitive damages as the Court may allow pursuant to 15 U.S.C. § 1681n(a)(2); and reasonable attorneys' fees and costs pursuant to 15 U.S.C. § 1681n(a)(3) from Defendant Arity Services, LLC.

163. As a result of each and every negligent noncompliance of the FCRA, Plaintiffs and FCRA Subclass Members are entitled to actual damages as the Court may allow pursuant to 15 U.S.C. § 1681o(a)(1); and reasonable attorneys' fees and costs pursuant to 15 U.S.C. § 1681o(a)(2) from Defendant Arity Services, LLC.

COUNT VII
CALIFORNIA CONSTITUTIONAL INVASION OF PRIVACY
(On Behalf of Plaintiff Jackson and the California Subclass Against All Defendants)

164. Plaintiff Jackson (for the purposes of this count, "Plaintiff"), individually and on behalf of the California Subclass, hereby repeats and incorporates by reference each preceding paragraph as if fully stated herein.

165. Plaintiff brings this claim on his own behalf and on behalf of each member of the California Class described above.

166. Article I, section I of the California Constitution states:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

Cal. Const. art I § 1 (emphasis added).

167. Plaintiff and California Class Members have an interest in precluding the dissemination and misuse of their driving data by Defendants, and using their personal property without observation, intrusion, or interference by Defendants.

168. Plaintiff and California Class Members had no knowledge and did not consent or authorize Defendants to obtain their driving data or to share it with third parties and with each other, let alone to use that data in determining insurance coverage and pricing.

169. Plaintiff and California Class Members enjoyed objectively reasonable expectations of privacy surrounding their driving telematics data.

170. Defendants' intrusion upon seclusion occurred the moment Defendants began tracking Plaintiff and California Class Members' driving data.

171. Defendants' conduct was intentional and intruded on Plaintiff's and California Class Members' use of their personal property.

172. Defendants' conduct was highly offensive to a reasonable person because they shared and/or sold the data for reports for auto insurance companies to influence Plaintiff's and California Class Members' insurance rates without their prior knowledge or consent.

173. As a direct and proximate result of Defendants' invasions of privacy, Plaintiff and California Class Members have suffered and will continue to suffer injury and damages, as alleged herein, including but not limited to overpayment for auto insurance services and decreased value of their driving telematics data.

174. Plaintiff and California Class Members seek all relief available for invasion of privacy claims under the California Constitution, including nominal damages and general privacy damages.

COUNT VIII
CALIFORNIA UNFAIR COMPETITION ACT, Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of Plaintiff Jackson and the California Subclass Against All Defendants)

175. Plaintiff Jackson (for the purposes of this count, "Plaintiff"), individually and on behalf of the California Subclass, hereby repeats and incorporates by reference each preceding paragraph as if fully stated herein.

176. Plaintiff brings this claim on his own behalf and on behalf of each member of the California Class described above.

177. Defendants are "persons" as defined by Cal. Bus. & Prof. Code § 17201.

178. Defendants violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

179. Defendants has engaged in "unlawful" business practices by violating California common law and California constitutional right to privacy.

180. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Class Members were injured and suffered damages, as alleged herein, including but not limited to invasion of privacy; overpayment for auto insurance services; and decreased value of their driving telematics data.

181. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Class Members' rights.

182. Plaintiff and California Class Members seek all monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices and reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5.

COUNT IX
VIOLATION OF THE CALIFORNIA WIRETAP ACT, Cal. Penal Code § 631
(On Behalf of Plaintiff Jackson and the California Subclass Against All Defendants)

183. Plaintiff Jackson (for the purposes of this count, "Plaintiff"), individually and on behalf of the California Subclass, hereby repeats and incorporates by reference each preceding paragraph as if fully stated herein.

184. At all relevant times, there was in full force and effect the California Wiretapping Act, Cal. Penal Code § 631.

185. The California legislature enacted the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*, including the Wiretapping Act, "to protect the right of privacy" of residents of California. Cal. Penal Code § 630.

186. The California legislature was motivated to enact CIPA by a concern that the "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.*

187. The California Wiretapping Act prohibits:

> any person [from using] any machine, instrument, [] contrivance, or in any other manner . . . [from making] any unauthorized connection, whether physically, electronically, acoustically, inductively, or otherwise, with any telegraph or telephone

> wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

188. Plaintiff's and California Class Members' specific user input events and choices on their mobile devices that are tracked by Defendants' Arity SDK communicates the user's affirmative actions, such as clicking a link, installing an app, selecting an option, or relaying a response, and constitute communications within the scope of the California Wiretapping Act.

189. The transmissions of information from Plaintiff's and California Class Members' mobile device sensors within Plaintiff's and California Class Members' mobile devices, and to the servers of third-party app developers, constitute communications within the meaning of the California Wiretapping Act.

190. Plaintiff and California Class Members are residents of California, and used their smartphones within California. As such, Defendants intercept, read, or attempt to read Plaintiff's and California Class Members' data, communications, and personal information in California.

191. On information and belief, Defendants use servers in California to intercept, track, process, or otherwise use Plaintiff's and California Class Members' data, communications, and personal information within California.

192. Defendants intercept Plaintiff's and California Class Members' communications while they are in transit within, to and from Plaintiff's and California Class Members' smartphones and the apps, app developers, and cellphone towers; Defendants transmit a copy of Plaintiff's and California Class Members' communications to themselves. Defendants use the contents of the communications to sell to third parties and in other methods for its own pecuniary gain.

193. Neither Defendants nor any other person informed Plaintiff and California Class Members that Defendants were intercepting and transmitting Plaintiff's and California Class Members' private communications. Plaintiff and California Class Members did not know Defendants

were intercepting and recording their communications, as such they could not and did not consent for their communications to be intercepted by Defendants and thereafter transmitted to others.

194. Defendants' Arity SDK constitutes a machine, instrument, contrivance, or other manner to track and intercept Plaintiff's and California Class Members' communications while they are using their smartphones.

195. Defendants use and attempt to use or communicate the meaning of Plaintiff's and California Class Members' communications by ascertaining their personal information, including their Personal Driving Data and places that they have visited, in order to sell Plaintiff's and California Class Members' personal information to third parties.

196. At all relevant times to this complaint, Defendants intercepted and recorded components of Plaintiff's and California Class Members' private telephone communications and transmissions when Plaintiff and California Class Members accessed Defendants' software via their cellular mobile access devices within the State of California.

197. At all relevant times to this complaint, Plaintiff and the California Class Members did not know Defendants were engaging in such interception and recording and therefore could not provide consent to have their Personal Data intercepted and recorded by Defendants and thereafter transmitted to others.

198. At the inception of Defendants' illegally intercepting and storing the Personal Driving Data, Defendants never advised Plaintiff or the other California Class Members that any part of this sensitive Personal Data would be intercepted, recorded, and transmitted to third parties.

199. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

200. Defendants' use of MAIDs and its SDK are both a "machine, instrument, contrivance, or . . . other manner" used to engage in the prohibited conduct at issue here.

201. At all relevant times, by using Defendants' MAID software and SDK as well as tracking Plaintiff's and California Class Members' geolocation and Personal Driving Data, Defendants intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiff and California Class Members on the one hand, and the specific sites and locations Plaintiff and California Class Members visited on the other.

202. At all relevant times, by using Defendants' geolocation tracking software technology, Defendants willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiff and putative class Members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

203. Plaintiff and California Class Members did not consent to any of Defendants' actions in implementing these wiretaps. Nor have Plaintiff or California Class Members consented to Defendants' intentional access, interception, reading, learning, recording, and collection of Plaintiff's and California Class Members' electronic communications.

204. Defendants violated Cal. Penal Code § 631 by knowingly accessing and without permission accessing Plaintiff's and California Class Members' devices in order to obtain their personal information, including their Personal Driving Data and location data, and in order for Defendants to share that data with third parties, in violation of Plaintiff's and California Class Members' reasonable expectations of privacy in their devices and data.

205. Defendants violated Cal. Penal Code § 631 by knowingly and without permission intercepting, wiretapping, accessing, taking, and using Plaintiff's and California Class Members' personally identifiable information and personal communications with others.

206. As a direct and proximate result of Defendants' violation of the Wiretapping Act, Plaintiff and California Class Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

207. Defendants were unjustly enriched by its violation of the Wiretapping Act. Pursuant to California Penal Code § 637.2, Plaintiff and California Class Members have been injured by Defendants' violation of the Wiretapping Act, and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief.

COUNT X
VIOLATION OF THE CALIFORNIA COMPUTER DATA ACCESS AND FRAUD ACT, Cal. Penal Code § 502
(On Behalf of Plaintiff Jackson and the California Subclass Against All Defendants)

208. Plaintiff Jackson (for the purposes of this count, "Plaintiff"), individually and on behalf of the California Subclass, hereby repeats and incorporates by reference each preceding paragraph as if fully stated herein.

209. The California legislature enacted the CDAFA with the intent of "expand[ing] the degree of protection afforded to individuals . . . from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). The enactment of CDAFA was motivated by the finding that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . unauthorized access to computers, computer systems, and computer data." *Id.*

210. Plaintiff's and California Class Members' smartphones constitute "computers" within the scope of the CDAFA.

211. Defendants violated the following sections of the CDAFA:

a. Section 502(c)(1), which makes it unlawful to "knowingly access[] and without permission . . . use[] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data;"

b. Section 502(c)(2), which makes it unlawful to "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network; and

c. Section 502(c)(7), which makes it unlawful to "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

212. Defendants knowingly accessed Plaintiff's and California Class Members' smartphones without their permission by including within the SDK that Defendants provides to app developers software that intercepts and transmits data, communications, and personal information concerning Plaintiff and California Class Members.

213. Defendants used data, communications, and personal information that they intercepted and took from Plaintiff's and California Class Members' smartphones to wrongfully and unjustly enrich itself at the expense of Plaintiff and California Class Members.

214. Defendants took, copied, intercepted, and made use of data, communications, and personal information from Plaintiff's and California Class Members' smartphones.

215. Defendants knowingly and without Plaintiff's and California Class Members' permission accessed or caused to be accessed their smartphones by installing, without Plaintiff's and California Class Members' consent, software that intercepts and/or takes data, communications, and personal information concerning Plaintiff and California Class Members.

216. Plaintiff and California Class Members are residents of California, and used their smartphones in California. Defendants accessed or caused to be accessed Plaintiff's and California Class Members' Personal Driving Data and personal information from California. On information and belief, Defendants uses servers located in California that allow Defendant to access and process the data, communications and personal information concerning Plaintiff and California Class Members.

217. Defendants were unjustly enriched by intercepting, acquiring, taking, or using Plaintiff's and California Class Members' data, communications, and personal information without their permission, and using it for Defendants' own financial benefit. Defendants have been unjustly enriched in an amount to be determined at trial.

218. As a direct and proximate result of Defendants' violations of the CDAFA, Plaintiff and California Class Members suffered damages.

219. Pursuant to CDAFA Section 502(e)(1), Plaintiff and California Class Members seek compensatory, injunctive, and equitable relief in an amount to be determined at trial.

220. Pursuant to CDAFA Section 502(e)(2), Plaintiff and California Class Members seek an award of reasonable attorneys' fees and costs.

221. Pursuant to CDAFA Section 502(e)(4), Plaintiff and California Class Members seek punitive or exemplary damages for Defendants' willful violations of the CDAFA.

COUNT XI
ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 Ill. Comp. Stat. §§ 505, *et seq.*
(On Behalf of Plaintiff Zimmerman and the Illinois Subclass Against All Defendants)

222. Plaintiff Zimmerman ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and reallege the preceding paragraphs as if fully alleged herein.

223. Defendants are each a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

224. Plaintiff and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

225. Defendants' conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

226. Defendants' deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Intercepting, collecting, using, and selling Plaintiff's and Illinois Subclass Members' Driving Data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Plaintiff's and Illinois Subclass Members' Driving Data to other third parties for their own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that Defendants and other parties collected, manipulated, used, and sold Plaintiff's and Illinois Subclass Members' Driving Data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of the Arity SDK with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of the Arity SDK and that it would protect the privacy of Plaintiff's and the Illinois Subclass Members' Driving Data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Plaintiff's and Illinois Subclass Members' Driving Data.

227. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Plaintiff's and Illinois Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Plaintiff's and Illinois Subclass Members' Driving Data without obtaining their consent. The fact that Defendants intercepted, collected, used, and sold Plaintiff's and Illinois Subclass Members' Driving Data was material to Plaintiff and Illinois Subclass Members. This is a fact that reasonable consumers would consider important when choosing to use a mobile app or in-vehicle app.

228. Plaintiff and Illinois Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants misrepresentations and omissions regarding the functionality of the Arity SDK, the security and privacy of their Driving Data, and their privacy in their own vehicles to their detriment.

229. Defendants intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on their misrepresentations and omissions.

230. In the course of its business, Defendants engaged in activities with a tendency or capacity to deceive.

231. Plaintiff and the Illinois Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

232. Defendants engaged in unfair and unconscionable conduct in violation of the Act by engaging in the conduct alleged herein, including by inducing Plaintiffs and Illinois Subclass Members to provide their Driving Data with knowledge that such data was obtained without

Plaintiff's and Illinois Subclass Members' consent, and further using, selling, and disseminating Plaintiff's and Illinois Subclass Members' Driving Data without their consent.

233. Defendants also violated the Act by knowingly taking advantage of Plaintiff's and Illinois Subclass Members' inability to reasonably protect their interests, due to their lack of knowledge regarding Defendants' practices, of which Defendants were aware.

234. Plaintiff's and the Illinois Subclass Members' Driving Data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff's and Illinois Subclass Members' Driving Data is in the possession of third parties—who have used and will use such data for their commercial benefit.

235. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable Driving Data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their Driving Data; and economic harm stemming from the exploitation of their Driving Data.

236. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT XII
ILLINOIS WIRETAPPING, ELECTRONIC SURVEILLANCE, AND INTERCEPTION OF COMMUNICATIONS LAW, 720 ILCS 5/14-1, *et seq.*
(On Behalf of Plaintiff Zimmerman and the Illinois Subclass Against All Defendants)

237. Plaintiff Zimmerman ("Plaintiff" for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

238. The Illinois Eavesdropping law, 720 ILCS 5/14-1, *et seq.*, prohibits, *inter alia*, any person from knowingly or intentionally "intercept[ing], record[ing], or transcrib[ing], in a surreptitious manner, any private electronic communication" without the consent of all parties. 720 ILCS 5/14-2(a)(3).

239. The Illinois Eavesdropping law also prohibits any person from using or disclosing "any information which he or she knows or reasonably should know was obtained" in violation of the Act,

unless such use or disclosure is done "with the consent of all of the parties." 720 ILCS 5/14-2(a)(5).

240. Defendants are each a "person" within the scope of the Illinois Eavesdropping law.

241. The data and transmissions within, to, and from Plaintiff's and Illinois Subclass Members' vehicles constitute "private electronic communications" as defined by 720 ILCS 5/14-1(e), as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic, or photooptical systems.

242. Plaintiff and Illinois Subclass Members have a reasonable expectation of privacy within their vehicles, and Plaintiff and Illinois Subclass Members reasonably expected privacy while driving their vehicles. Further, there is a reasonable expectation that the interactions between a driver and their vehicle, *i.e.*, their personal Driving Data, are private.

243. As alleged herein, Defendants have intercepted, in real time, contemporaneously, and as they were transmitted, the contents of private electronic communications, and diverted those communications to itself without consent.

244. Defendants intercepted these data transmissions by diverting them to their own servers, unbeknownst to Plaintiff and Illinois Subclass Members.

245. As detailed herein, the electronic communications detailed above that Defendants intercepted are tied to individual drivers and vehicles, and not anonymized.

246. In further violation of the Illinois Eavesdropping law, Defendants intentionally disclosed or endeavored to disclose to third parties the contents of the private electronic communications described above while knowing or having reason to know that the information was obtained through the interception of the private electronic communications.

247. In further violation of the Illinois Eavesdropping law, Defendants intentionally used or endeavored to use the contents of the communications described above knowing or having reason to know that the information was obtained through interception in violation of the Act.

248. Defendants have disclosed and used the contents of the communications described above by selling consumers' personal Driving Data to the third parties, for its own financial and commercial benefit, obtaining substantial profit.

249. In violation of the Illinois Eavesdropping law, Defendants intentionally disclosed,

used, or endeavored to use disclose to third parties the contents of Plaintiff and Illinois Subclass Members' private electronic communications intercepted by Defendants while knowing or having reason to know that the information was obtained through the interception of the communications in violation of the Illinois Eavesdropping law.

250. Specifically, Defendants intentionally disclosed or endeavored to disclose Plaintiff and Illinois Subclass Members' detailed Driving Data to various auto insurance companies.

251. Defendants further used the information derived from Plaintiff's and Illinois Subclass Members' private electronic communications to create products they market, license, and sell, including so-called driving scores, risk ratings, and access to databases containing Plaintiff's and Illinois Subclass Members' Driving Data. Defendants also used the information derived from the communications described above in aggregate fashion to create their telematics exchange, develop risk models, and other products they market and sell.

252. Defendants knew or should have known that the detailed driving information they used and sold was captured in violation of the Illinois Eavesdropping law for the following reasons, among others that will become known through discovery:

a. the numerous, obvious consent and privacy challenges to the collection of Driving Data that Defendants acknowledged in writing and in presentations;

b. the opaque disclosures in Defendants various terms and policies, which did not operate as a reasonable basis for inferring consumer consent to share the information with Defendants;

c. the sheer volume of data Defendants were receiving versus from other manufacturers;

d. the lack of public knowledge about Defendants' collection and sharing practices until at least 2024;

e. that fact that Defendants continued to collect after it was publicized that collection was secret/happening without consent or knowledge; and

f. the nature of the data as such that it had to be obtained via a wiretap.

253. Plaintiff and Illinois Subclass Members did not consent or otherwise authorize

Defendants to intercept, disclose, or use their communications.

254. As a result, Plaintiff and Illinois Subclass Members have suffered harm and injury due to the interception, disclosure, and/or use of communications containing their private and personal information.

255. Pursuant to 720 ILCS 14-6, Plaintiff and Illinois Subclass Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Eavesdropping law and are entitled to: (1) damages, in an amount to be determined at trial; (2) punitive damages; (3) injunctive relief prohibiting Defendants from further eavesdropping; and (4) reasonable attorneys' fees and other litigation costs reasonably incurred.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiffs as class representatives;

b. For permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

c. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

d. For an award of actual damages and compensatory damages, in an amount to be determined;

e. For an award of pre-judgment and post-judgment interest as allowed by law;

f. For an award of costs of suit and attorneys' fees, as allowable by law; and

g. Such other and further relief as this court may deem just and proper.

IX. JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: January 27, 2025

Respectfully submitted,

By: */s/ Lesley E. Weaver*

Lesley E. Weaver (SBN 191305)
lweaver@bfalaw.com
Anne K. Davis (SBN 267909)
adavis@bfalaw.com
Joshua D. Samra (SBN 313050)
jsamra@bfalaw.com
BLEICHMAR FONTI & AULD LLP
1330 Broadway, Suite 630
Oakland, California 94612
Tel.: (415) 445-4003
Fax: (415) 445-4020

Gregory S. Mullens (*pro hac vice* forthcoming)
gmullens@bfalaw.com
BLEICHMAR FONTI & AULD LLP
75 Virginia Road, 2nd Floor
White Plains, New York 10603
Tel.: (415) 445-4006

Sabita J. Soneji (SBN 224262)
ssoneji@tzlegal.com
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, California 94612
Tel.: (510) 254-6808

Shana Khader (*pro hac vice* forthcoming)
skhader@tzlegal.com
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Ave. NW, Suite 1010
Washington, D.C. 20006
Tel.: (202) 973-0900

Counsel for Plaintiffs and the Proposed Class